

Notice of Allowability

Application No.

10/683,554

Examiner

HOSUK SONG

Applicant(s)

LIANG, YUNG CHANG

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to Amendment filed on 6/1/07.
2. ☒ The allowed claim(s) is/are 1,2,4,5,7 and 8.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date 10683554
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

HOSUK SONG
PRIMARY EXAMINER

INNOCULATION OF COMPUTING DEVICES AGAINST A SELECTED COMPUTER VIRUS

CROSS REFERENCE TO RELATED APPLICATIONS

This application takes priority under 35 U.S.C. §119(e) of U.S. Patent Application No 60/481,313 filed August 29, 2003 (Attorney Docket No.: TRNDP009P) naming Liang et al. as inventor(s) entitled "VIRUS MONITOR AND METHODS OF USE THEREOF" which is also incorporated herein by reference for all purposes. This application is also related to the following co-pending U.S. Patent applications, which are filed concurrently with this application and each of which are herein incorporated by reference, (i) U.S. Patent Application No. 10/684330 (Attorney Docket No.: TRNDP009), entitled "VIRUS MONITOR AND METHODS OF USE THEREOF" naming Liang et al as inventors; (ii) U.S. Patent Application No. 10/683582 (Attorney Docket No.: TRNDP010), entitled "AUTOMATIC REGISTRATION OF A VIRUS/WORM MONITOR IN A DISTRIBUTED NETWORK" naming Liang et al as inventors; (iii) U.S. Patent Application No. 10/683579, (Attorney Docket No.: TRNDP011), entitled "NETWORK TRAFFIC MANAGEMENT BY A VIRUS/WORM MONITOR IN A DISTRIBUTED NETWORK", naming Liang et al as inventors; and (iv) U.S. Patent Application No. 10/683874 (Attorney Docket No.: TRNDP012), entitled "ANTI-VIRUS SECURITY POLICY ENFORCEMENT", naming Liang et al as inventors; (v) U.S. Patent Application No. 10/683873 (Attorney Docket No.: TRNDP014), entitled "NETWORK ISOLATION TECHNIQUES SUITABLE FOR VIRUS PROTECTION", naming Liang et al as inventors; and (vi) U.S. Patent Application No. 10/683584 (Attorney Docket No.: TRNDP015), entitled

[0054] Accordingly, FIG. 8 illustrates a virus monitor 800 as one possible implementation of virus monitor 102. Accordingly, the virus monitor 800 includes a traffic controller 802 coupled to network 100 by way of a network interface 804 that includes an intruder detection system (IDS) module 806 for evaluation of potential intruder attacks described in co-pending U.S. Patent Application No. 10/411665, Attorney Docket No. 87152491-002027 entitled, "MULTILEVEL VIRUS OUTBREAK ALERT BASED ON COLLABORATIVE BEHAVIOR" by Liang et al filed 4/10/03 which is incorporated by reference herein in its entirety for all purposes. Such intruder based attacks include a Denial of Service (DoS) attack whereby a large number of requests are made to a particular server computer within a small period of time resulting in the attacked server computer being unable to provide access to other, legitimate, requestors. The IDS module 806 determines an associated alert level based on the volume of the data traffic flow at the virus monitor 800 in a unit time interval which is designated as being abnormal if the volume of the data traffic flow is larger than a predetermined value in a predetermined time period.

[0055] Typically, a host base IDS (not shown) sets an alert threshold very high in order to reduce the rate of false alarms in detecting viruses, which may cause inefficiencies and inflexibilities in dealing with virus outbreaks. In contrast, the collaborative anti-virus system adopts multilevel alert thresholds, with the highest alert thresholds being comparable to those of a host base IDS. Below the highest threshold, at least two lower thresholds are maintained in grouping activities at